The Center for Information Systems
Security Studies and Research

Technical Report NPS-CS-05-002

High Assurance Testbed For Multilevel Interoperability

2004 Developments

Cynthia E. Irvine, Thuy D. Nguyen, Timothy E. Levin
October 2004

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
High Assurance Multilevel Testbed 2004 Developments	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,The Center for Information Systems Security Studies and Research,Monterey,CA,93943-5000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**10**	

ACKNOWLEDGMENTS

This work was sponsored in part by the Office of Naval Research grants N001403AF00002, N0001403WX21224, and N001404WR20357.
This work was funded in part by the National Reconnaissance Office under funding document E338270.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research or the National Reconnaissance Office

1 Introduction

Current military and intelligence operations utilize a variety of specialized (often called "stove-piped") systems to provide I/O and computing. Access to and controlled sharing of information from various networks operating at different classifications (e.g., NIPRNET, SIPRNET, JWICS, and COWANS) is difficult in ad hoc operational networks. To address the exchange of information in command and control and intelligence systems in the emerging Global Information Grid (GIG), such as the Theater Battle Management Core System (TBMCS), requires support for high assurance authentication and multilevel capabilities.

These requirements provide the impetus for the creation of two complementary research efforts: the Monterey Security Architecture (MYSEA) project and the Trusted Computing Exemplar (TCX) project. The objective of the MYSEA project is to explore and develop a high assurance heterogeneous distributed operating environment that is capable of enforcing multilevel security policies while maintaining support for existing applications and unmodified commodity client systems [1]. The purpose of the TCX project is to provide an openly distributed worked example of how high assurance trusted components could be constructed [2]. The TCX reference implementation, i.e., the TCX Separation Kernel, will be developed in accordance with the Common Criteria evaluation methodology [3] and will be used as the underlying trusted foundation for two MYSEA trusted components, the Trusted Path Extension (TPE) and Trusted Channel Module (TCM).

Synergistically, the purpose of the Multilevel Security (MLS) Testbed project is to create a stable testing environment for experimentation in high assurance security services being developed in the MYSEA and TCX projects. These include assured authentication and trusted path access to security critical functions, MLS services and secure single level connections to existing classified networks.

The MLS Testbed project is an on-going effort supported by multiple sponsors. This document describes the progress made in FY2004 that includes the construction of the MLS Testbed and the functional testing of the security services currently supported by the MYSEA server.

2 Technical Overview

The project mission is to create an evolving testbed for a distributed multilevel secure architecture such as MYSEA that combines protection against cyber attacks with a hardened foundation for coalition operations. The goal is to demonstrate how U.S. participants can use a single workstation for multilevel access to U.S. and coalition WANS at different classification levels. Leveraging previous MYSEA R&D results, demonstration scenarios running on the MLS Testbed show that it is feasible to afford popular desktop applications, e.g. the Microsoft Office suite, to clients in a MLS/Multiple Security Level (MSL) environment and to provide operators within a community of interest network (COIN) with web-based views of multilevel information.

2.1 Project Background and Benefits

2.1.1 Background

As the intelligence community and military make advances toward new information architectures intended to provide connectivity and information sharing on an unprecedented scale, a number of challenges must be addressed. Today, Internet users are plagued by daily barrages of spam in their e-mail boxes, while the Internet as a whole is disrupted by rapidly propagating, automated attacks that exploit system vulnerabilities. A perceived requirement for use of commodity software familiar to home users, but lacking the robustness and security protections required for industrial-grade critical missions has further exacerbated weaknesses in the information infrastructure. Without improved security measures in tandem with improved bandwidth, the realization of useable and defensible information infrastructures may be only a chimera.

Among the most important of the security mechanisms required for the shared vision is strong and secure authentication. The unspoofable binding between users and the system entities that act on their behalf must be established through mechanisms by which users have a positive connection to trusted elements in the system supporting security critical activities. The trustworthy connection presented by the system is known as the *trusted path*: it provides confidence that neither the system nor the user is being spoofed. Such a high confidence trusted path is needed for networks intended to achieve the highest evaluation classes under current criteria guidance. Trusted path mechanisms will provide enabling technology for Navy operations requiring information classified at different sensitivity levels and involving coalition forces.

2.1.2 Benefits

The MLS Testbed provides an evolving simulated distributed MLS environment that will permit experimentation in the following research areas:

- Secure connections to classified networks
- Secure reuse of commercial-off-the-shelf (COTS) and legacy hardware and software components
- Application of high assurance security technology to legacy components
- Interoperability with the DoD PKI infrastructure
- Centralized security management within the context of a distributed environment
- Secure integration of multilevel security with existing sensitive networks
- High assurance trusted path techniques for managing access to classified networks
- Flexibility to incorporate new technologies

The notion that clients can be heterogeneous will support efforts involving a variety of partners, which in turns will promote MLS awareness in the commercial sector.

2.2 MLS Testbed Design Overview

The 2005 Testbed design is shown in Figure 1. Using mostly COTS components, the Testbed provides a demonstration environment for the following functionalities:

- True multilevel access to data at multiple levels of security using a single commercial workstation
- Single-level-at-a-time access to sensitive single level networks (i.e., simulated NIPERNET and SIPERNET) using a single commercial workstation
- Access to heterogeneous operating systems, hardware components and applications
- Use of a high assurance server as locus of high assurance security policy enforcement
- Use of hand held appliances for trusted path
- Controlled interaction of disparate coalitions and enclaves

Figure 1. 2005 MLS Testbed Design

Although Figure 1 shows one MLS server, the MYSEA design supports the use of a federation of MLS servers to provide better performance, scalability and reliability. The MYSEA server enforces a unified mandatory access control security policy based on the Bell-LaPadula [4] confidential policy and the strict Biba [5] integrity policy. The Trusted Path Extension (TPE) device is a trusted component responsible for providing a secure interface for user interaction with selected MYSEA Server security functions. After a successful login and session level negotiation via the trusted path, an MLS LAN user can access any data at the MYSEA server that is allowed by the security policy. The current MYSEA security policy allows reading information that is at the same or lower in sensitivity than the negotiated session level. All information written will be labeled at the negotiated session level.

Similarly, the Trusted Channel Module (TCM) device is a trusted component responsible for providing secure identification of single level networks connected to the MYSEA server. When accessing the MYSEA server via the TCM, users on a single level network can only access data on the MYSEA server at the classification level assigned to the corresponding TCM.

The Tarantella/enView server is used to provide to MLS LAN clients, via an integrated portal view, web-based access to applications that run on different server platforms (Windows, Unix, Linux). This will allow the use of standard web browsers to access proprietary applications on the simulated legacy networks, e.g., Word or PowerPoint. The inclusion of web-enabling technology is part of the MYSEA's thin-client migration strategy.

The Command and Control Personal Computer (C2PC) system, a battlefield situational awareness tool, is used in the Testbed to demonstrate the ability to support legacy mission-critical applications. The C2PC REPEAT track simulator acts as a Global Command and Control System (GCCS) server that, in a real operational environment, would feed tactical information to the C2PC Gateway and C2PC Clients. The C2PC Gateway is the conduit between the GCCS server (i.e., REPEAT track simulator) and the C2PC Clients. It provides tactical track data received from the GCCS server to the C2PC Clients and forwards track updates from the C2PC Clients to the GCCS server. In the demonstration, the C2PC Client is a Windows application hosted on an MLS LAN client workstation, which displays the tactical map window.

Both military-grade Type 1 encryption devices and commercial VPN appliances are used in the Testbed to simulate the protected end-to-end communication between the MLS controlled environment and remote single level networks.

3 MLS Testbed

3.1 Network Topology

In 2004, the CISR team constructed the MLS testbed as shown in Figure 2. The current testbed differs in several ways from the 2005 Testbed design discussed in Figure 1. Since the development of the Trusted Channel Module (TCM) component is not yet completed, the SECRET and COALTION segments are separately connected to the MYSEA server via two single level network interfaces instead of being multiplexed onto one MLS interface.

Another difference is the configuration of the C2PC system. Enhancements to the MYSEA server to support C2PC proxy services are required in order to implement the C2PC configuration depicted in Figure 1, i.e., C2PC Client application running locally on an MLS LAN workstation. Since these enhancements are not yet available, the C2PC Client application is hosted on a remote server and accessed by the MLS LAN client via Tarantella/enView.

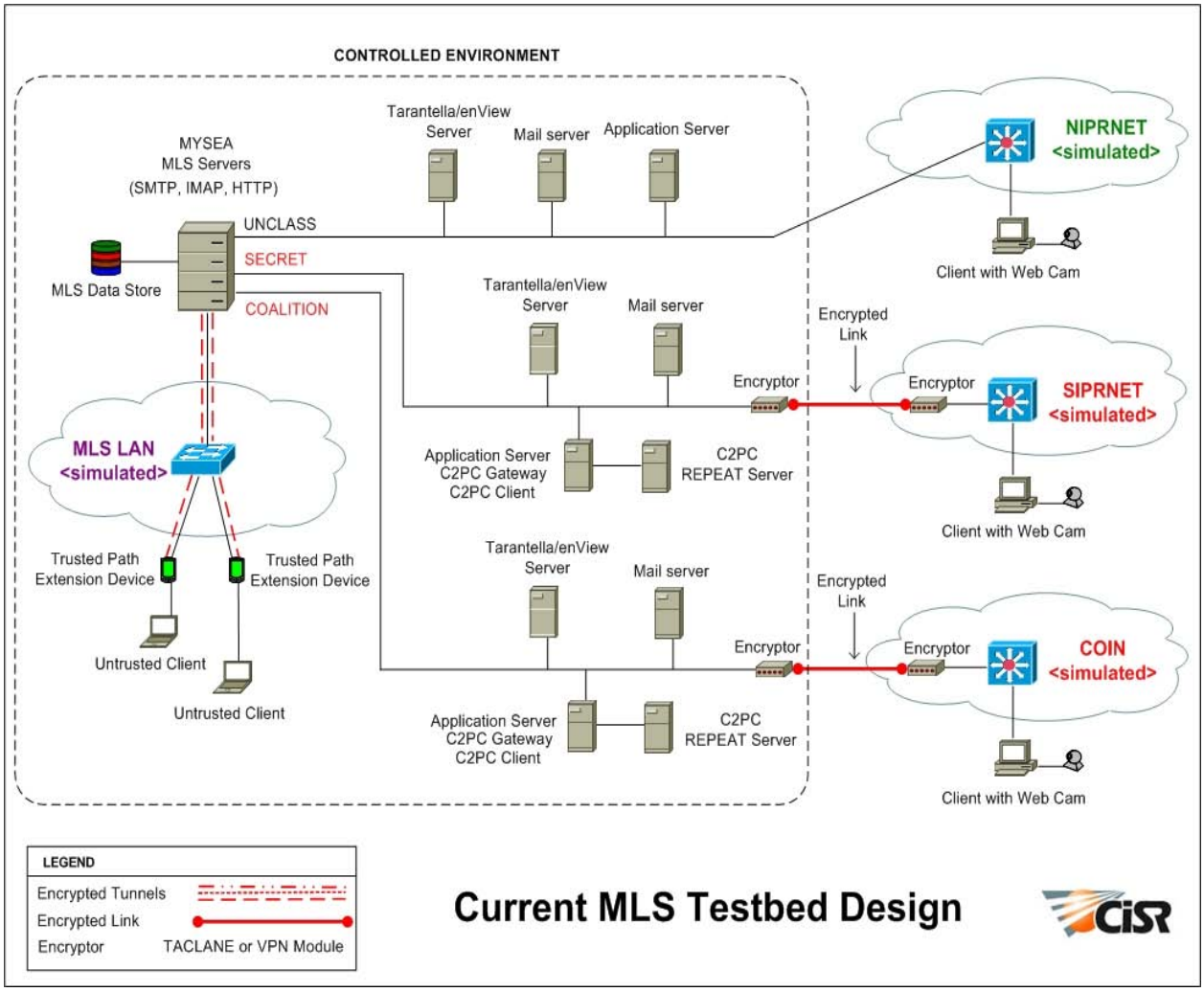

Figure 2. Current MLS Testbed Design

3.2 Hardware Components

The Testbed consists of 35 machines, categorized as follows:

Special Purpose Equipment:

- MLS server: 1 (DigitalNet XTS-400)
- Handheld TPE devices: 2 (iPAQ Pocket PC)

Commercial-Of-The-Shelf Equipment:

- Servers: 14 (9 rack-mounted platforms, 5 desktops)
- Laptop clients: 5
- VPN appliances: 4
- Network switches: 5

Government Furnished Equipment:

- TACLANE (Type 1 encryptor) devices: 4

Hardware Acceptance Test Procedures were established and used to verify that each hardware element worked properly before being used in the actual Testbed.

3.3 Software Components

The following set of software from different vendors is used in the Testbed to simulate a heterogeneous operating environment.

- *Trusted Operating System*: DigitalNet Secure Trusted Operating System (STOP). The XTS-400 running STOP was evaluated at the Common Criteria EAL-4+ level and is currently being evaluated at the EAL-5+ level [6].

- *Operating Systems*: RedHat Linux, Microsoft Windows 2000 server, Microsoft Windows XP and Familiar Project Linux

- *MLS Application (running on the MYSEA server)*: Apache-like web server

  Linux Applications: PostgreSQL, Apache web server, Edge Technologies enPortal, Tarantella Enterprise 3, imapd and sendmail

- *Windows Applications*: Microsoft Terminal Services, Microsoft Office, Microsoft Project, Internet Explorer, C2PC Gateway, C2PC Client, REPEAT 2004–RepeatWinXR and Creative WebCam PROeX

A set of software configuration procedures was written and used to set up and maintain the Testbed.

4 Functional Testing

4.1 MLS Services

The MYSEA server in the testbed is currently configured to run an Apache-like web server. After a successful login to the MYSEA at an authorized session level via the TPE, a user on the MLS LAN can view web pages at the same or lower sensitivity level. Multilevel email will be available in the near future.

4.2 MSL Services

The following COTS applications have been tested and are being used in the Testbed via the Tarantella/enView integrated portal interface:

- Microsoft Office (Word, PowerPoint, Excel, Access)
- Microsoft Project
- Microsoft Outlook Express

- Creative PC-Cam Center (running as a standalone client application)

4.3 Transmission Security Services

Two pairs of high assurance TACLANE network encryptors are used to simulate the encrypted channels required to protect data transmissions between networks that are geographically separated, i.e., between the MYSEA controlled environment and the SIPRNET and COIN segments. The TACLANE devices are keyed with dummy test keys and are physically protected while not in use.

For day-to-day testing, two pairs of Cisco IPsec VPN devices are used in place of the TACLANE devices. The IPsec attributes used to set up the VPN channels are as follows:

- Hash algorithm: HMAC-SHA1
- Encryption algorithm: 3DES-CBC
- Host authentication method (for Security Association establishment): pre-shared secret
- Security protocol: IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP) with ESP authentication
- Mode of operation: tunnel mode
- Key management: automated using IKE

5 Future Plans

In the next year we expect to incorporate into the Testbed new MYSEA features as well as the following MYSEA functionalities that are currently under development:

- MLS services: IMAP and SMTP applications, NFS and SAMBA support
- "Stateless" MLS LAN clients running embedded XP
- Support for running remote client applications on the MYSEA server
- Proof-of-concept TCM prototype
- TPE hardware migration to newest iPAQ model

In addition to accommodating new MYSEA and TCX technologies and requirements, we will explore the integration of the MLS Testbed into the GIG architecture. We also plan to conduct performance analyses of the Testbed.

References

[1] Irvine, Cynthia E., Levin, Timothy E., Nguyen, Thuy D., Shifflett, David, Khosalim, Jean, Clark, Paul C., Wong, Albert, Afinidad, Francis, Bibighaus, David, and Sears, Joseph, "Overview of a High Assurance Architecture for Distributed Multilevel Security," *Proceedings of the 2004 IEEE Systems Man and Cybernetics Information Assurance Workshop*, West Point, NY, June 2004, pp. 38-45.

[2] Irvine, Cynthia E., Levin, Timothy E., Nguyen, Thuy D., and Dinolt, George W., The Trusted Computing Exemplar Project, *Proceedings of the 2004 IEEE Systems Man and Cybernetics Information Assurance Workshop*, West Point, NY, June 2004, pp. 109-115.

[3] Common Criteria Project Sponsoring Organisations, Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-001, Version 2.2, January 2004.

[4] D.E. Bell and L. LaPadula, "Secure Computer System: Unified Exposition and Multics Interpretation," *Tech. Rep. ESD-TR-75-306*, MITRE Corp., Hanscom AFB, MA, 1975.

[5] K.J. Biba, "Integrity Considerations for Secure Computer Systems," *Tech. Rep. ESD-TR-76-372*, MITRE Corp., 1997.

[6] Security Target Version 1.7 for XTS-400 Version 6.0.E, http://niap.nist.gov/cc-scheme/st/ST_VID3012-ST.pdf, DigitalNet Government Solutions, LLC, March 2004.